International Journal of Research in Advent Technology, Vol.2, No.10, October 2014
E-ISSN: 2321-9637

Design and Analysis Of Enhanced Group Key Management Schemes in MANET

M.Marimuthu[1], Dr.R.Gunavathi[2]
M.Phil. Scholar, Department of Computer Science,
Head of the department, Department of PG Computer Applications, STC, Tamilnadu
Email: jeevan15887@gmail.com[1], Email: gunaganesh2001@gmail.com[2]

Abstract- In this day of electronic communication and with the ever-increasing worldwide usage of the Internet, securing sensitive information such as credit card numbers, passwords, government secrets, medical information etc. is becoming increasingly important. In the information age, cryptography enables us to store sensitive information or transmit it across insecure networks like internet, so that it cannot be read by anyone except the intended recipient. Among many issues of cryptography, exchange of keys among the communication party is one of the great challenges. There are various key management schemes are available in cryptography to solve the said problem. This research is mainly concerned about the study of various group key management schemes in MANET. The major categories of group key management schemes are contributory and distributive. The Autonomous key management (AKM) is one of the symmetric algorithm with a large number of nodes based on a hierarchical structure to provide flexibility and adaptively. The AKM can use any asymmetric scheme such as RSA to generate the pubic keys. In this research, the process of AKM is enhanced by replacing RSA by Elliptic Curve Cryptography (ECC) algorithm. From the simulated results, it is found that the AKM uses ECC is better than the existing algorithms.

Index terms: cryptography, MANET, group key management, AKM, RSA, ECC algorithm.

1. INTRODUCTION

In the information age, cryptography enables us to store sensitive information or transmit it across insecure networks like internet, so that it cannot be read by anyone except the intended recipient. Based on the number of keys used in the process of encryption and decryption, cryptography is characterized in two types such as symmetric key and asymmetric key cryptography. Among many issues of cryptography, exchange of keys among the communication party is one of the great challenges. There are various key management schemes are available in cryptography to solve the said problem.

The wireless and dynamic nature of mobile ad hoc networks (MANET) leaves them more vulnerable to security attacks than their wired counterparts. The nodes in this network may join and leave at any instance and it is very difficult to keep the groups in safe. A group can be static or dynamic. A dynamic group allows the exclusion of members as well as the addition of new members. Key management for dynamic groups can provide forward secrecy, when members that leave the group are unable to compute future group keys, and backward secrecy, when new group members are unable to compute old group keys.

The major categories of group key management schemes are contributory and distributive. Distributive scheme is further classified as public key schemes and symmetric key schemes. The Autonomous key management (AKM) is one of the symmetric algorithm with a large number of nodes based on a hierarchical structure to provide flexibility and adaptively. The AKM can use any asymmetric scheme such as RSA to generate the pubic keys. In this paper, the process of AKM is enhanced by replacing RSA by Elliptic Curve Cryptography (ECC) algorithm.

1.1 cryptography

Cryptography can be defined as the process of making information indecipherable to all except those who are the intended recipients of such information. Through various methods of cryptography, data can be safely transmitted without the threat of the information being intercepted and subsequently, compromised. Data that can be read and understood without any special measures is called plaintext.

The method of plaintext in such a way as to hide its substance is called encryption. Encrypting

plaintext results in unreadable form called cipher text. The process of reverting cipher text to its original plaintext is called decryption. The process of encryption and decryption is depicted in the following figure 1.

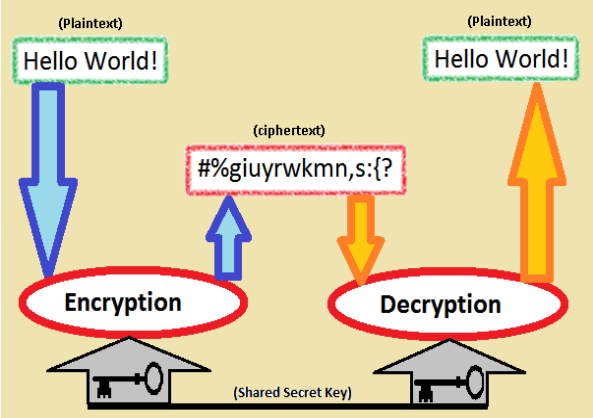

Figure 1: Encryption and Decryption

1.2 Types of cryptography

Based on the number of keys used in the process of encryption and decryption, cryptography is characterized in two types: (i) Symmetric key cryptography (ii) Asymmetric key cryptography.

First and foremost model of cryptosystem is symmetric key cryptosystem. In this system both the sender and receiver use the same key to encrypt and decrypt the message. Key must choose carefully, distributed securely among the communication parties. Some of the known symmetric algorithms are Advanced Encryption Standard (AES), Blow fish, Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), RC6 etc. Even though these algorithms are good enough, they are not able to provide service other than confidentiality. Apart from this, symmetric model has some problems like Key Distribution, Key Management, and the number of keys.

To overcome the above said problem, Asymmetric cryptosystem also known as public key cryptosystem was introduced. It uses a pair of keys, designated as public key and private key. The public keys encrypt the message, only the corresponding private key permits to decrypt it. The standard public key algorithms are Digital Signature Algorithm (DSA), ElGamal, RSA (Rivest Shamir Adelman), Diffie-Hellman (Merkle) key exchange, Elliptic Curve Cryptography (ECC).

1.3 role of key in cryptography

Any cryptographic algorithm works in combination with a key to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key. Without a key, the algorithm would produce no useful result. A *key* is a value that works with a cryptographic algorithm to produce a specific cipher text and keys are basically big numbers.

Key size is measured in bits; the number representing a 1024 bit key is huge. Bigger the key, the more secure the cipher text. While the public and private keys are mathematically related, it's very difficult to derive the private key given only the public key; however deriving the private key is always possible given enough time and computing power. This makes it very important to pick the keys of the right size, large enough to be secure, but small enough to be applied fairly quickly. In order to use the key in the cryptographic process, key need to stored, exchanged and used.

1.4 Mobile Ad Hoc Networks (MANET'S)

In areas where there is little communication infrastructure or the existing infrastructure is inconvenient to use, wireless mobile users may still be able to communicate through the formation of mobile ad hoc networks. A mobile ad hoc network, or simply MANET, is a collection of wireless mobile hosts that form a temporary network without the aid of any centralized administration or support.

In such a network, each mobile node operates not only as a host but also as a router, forwarding packets for other mobile nodes in the network that may be multiple hops away from each other. Possible applications of MANETs include: soldiers relaying information for situational awareness on the battlefield; business associates sharing information during a meeting; attendees using laptop computers to participate in an interactive conference; emergency disaster relief personnel that are coordinating efforts at sites of fires, hurricanes, or earthquakes.

2. RELATED WORKS

URSA is a localized key management scheme proposed by Luo, Kong, and Zerfos in their paper "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks"[33]. The difference between URSA and SRP is that in URSA, all nodes are servers and are capable of producing a partial certificate, while in SRP only server nodes can produce certificates. Thus, certificate services are distributed to all nodes in the network. This scheme

generates communication delay, search failure, and degrades the system security. It reduces system security, especially when nodes are not well-protected because an attack can easily locate a secret holder without much searching and identifying effort.

Partially Distributed Threshold CA Scheme was discovered by Zhou, L. and Hass,Z. When the mobile ad-hoc network is constructed, this scheme is using the concept of CA distribution in threshold fashion[26]. Security services like off line authentication, great intrusion tolerance, and trust management by CA (certification authority) are provided by Z&H asymmetric key management scheme.

In the self-organized network each mobile node acts as a distinct CA.SOKS was disclosed by Capkun, S., Buttya, L., and Hubaux, P[34]. It has poor scalability and poor resource efficiency but having the off line authentication and limited intrusion detection security services. SOKS having high intermediates

Cluster Based Composite Key Management is disclosed by R.PushpaLakshmi and A. Vincent Antony Kumar in 2010. This scheme takes the concept of off-line CA, mobile agent, hierarchical clustering and partial distribute key management. Public key of the members are maintained by cluster head that reduces the problem of storage in PKI. Overview of cluster based composite key management scheme it supports network extendibility through hierarchical clustering. This model saves network bandwidth and storage space.

Zone-Based Key Management Scheme using ZRP (Zone Routing Protocol). This model is proposed by ThairKhdour and Abdullah Arefin 2012, in this model for each mobile node zone is defined [15]. Some pre-defined number is allocated to each mobile node which depends on the distance in hops. Symmetric key management is used by mobile node only for intra or inside zone radius. Without depends on clustering mobile node uses asymmetric key management for inter-zone security. It efficient way to making the public key without losing the capability encryption operations and high storage cost.

3. GROUP KEY MANAGEMENT SCHEMES

Group key is a single key which is assigned only for one group of mobile nodes in MANET. For establishing a group key, group key is creating and distributing a secret for group members. There are classified in several ways. The main categories are Contributory Schemes and Distributive Schemes. Centralized, in which the controlling and rekeying of group is being done by one entity. Decentralized, more than one entity is responsible for making, distributing and rekeying the group key.

3.1 Contributory schemes

These are characterized by the lack of a trusted third party responsible for generation and distribution of the cryptographic keys. Instead, all communicating parties cooperate to establish (i.e., “agree” upon) a secret symmetric key. The number of participants ranges from two parties (establishing a pair wise key) to many parties (establishing a group key). Although not necessarily designed with adhoc networks in the contributory approach of collaboration and self-organization may seem to fit the nature of ad hoc networks. Only one of these was designed specifically for ad hoc networks.

3.2 Distributive Schemes

Distributive, where each key originates from a single node. The nodes cooperate during key distribution, but any key originates from a single source. Distributive schemes may also be centralized, but can also be distributed. Each node generates a key and to distribute to others. It involves one or more trusted entities and comprise both public key systems and symmetric systems. The Distributive category is divided into symmetric and public schemes. Public key schemes include traditional certificate-based and identity based schemes. The symmetric schemes are classified as either MANET schemes or WAN wireless sensor networks schemes. WSN represents a new class of adhoc networks with more constrained nodes than traditional MANET.

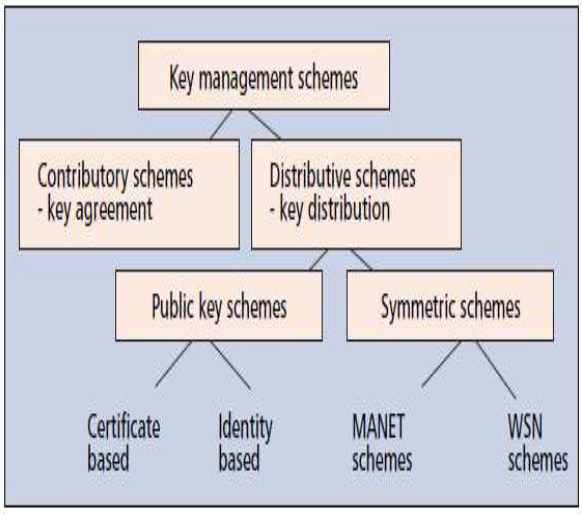

Figure 2: Classification of Key Management Schemes

4. COMPARISON OF CONTRIBUTORY AND DISTRIBUTIVE SCHEMES

4.1. Summary of the Contributory Schemes

Contributory approach at first glance may seem to fit the self-organizing nature of adhoc networks none of the contributory schemes are good for key management in ad hoc networks D-H, ING, and H&O can be skipped due to missing authentication. They are vulnerable to MIM attacks. B-D and CLIQ can be left out they have an inherent survivability problem with the dependency on reliable multicasting. A-G fails on scalability and robustness due to the dependency upon node ordering and availability of all nodes during group changes.

4.2. Summary of Public Schemes

The Capabilities of the public key schemes are summarized in Table 2. IBC-K, making certificate an exchange superfluous is an interesting for adhoc networks. The reliance of a PKG makes it best suited for SAD operations. Depending on whether or not the security policy demands centralized trust management, IBC-K or COMP/UBIQ fits better in the case of MAD operations.

4.3 Summary of Symmetric Schemes

It gives an overview of the capabilities of the distributive symmetric key management schemes. The WSN key management schemes generally assume static nodes, mass deployment, or designed to establish pairwise keys. Their aim and assumptions render them inapplicable for protection of routing information in traditional ad hoc networks with mobile nodes. PSGK extended with S-HEAL or LKH for revocation, appear to be the most promising alternatives to symmetric schemes.

The summary of all the above said or discussed schemes are provided in the following tables.

		D-H	ING	B-D	H&O	A-G	CLIQ
Characteristics		Two parties	Logical ring of nodes during D-H key agreement	Reduce the number of rounds to 3 by reliable multicasting	Reduce the number of rounds from n to d ($n = 2^d$) by arranging nodes into hypercube	Password authenticated H&O	Group changes through reliable multicast from group controller
Applicability	Aim	P	G	G	G	G	G
	Net	S.O.	S.O.	Planned	S.O.	S.O.	S.O.
Security	Authentication	No/None	No/None	Public key	No/None	Password	No/None
	Intrusion tolerance	Yes	No/None	No/None	No/None	No/None	No/None
	Trust Management	Nodes	No/None	CA	No/None	Organizer	GC
	Vulnerabilities	MIM	O, MIM, Byzantine Behavior	O, Byzantine Behavior	O, MIM, Byzantine Behavior	O, Byzantine Behavior	O, MIM, Byzantine behavior
Robustness	Availability assumptions	Peer	Ring O	O + RM	Hypercube O	Hypercube O	O + GC + RM
	Byzantine behavior & Faulty nodes	Yes	No/None	No/None	No/None	No/None	No/None
	Group changes	N/A	Re-key	Re-key	Re-key	Re-key	Re-key
Scalability		Poor	Poor	Poor	Poor	Poor	Poor

G: Group Key (symmetric), GC: Group Controller, MIM: Man-in-the-middle, O: node ordering, P: Pairwise symmetric key, RM: reliable multicast ,S.O.: self organizing

Table 1: Summary of Contributory Schemes

		Z-H	MOCA	SEKM	UBIQ	AKM	PGP-A	COMP	MOB	IBC-K
Characteristics		Group of servers forms Threshold CA	Most powerful nodes form Threshold CA	Threshold CA servers form multicast group	All nodes part of threshold CA	"Hierarchical UBIQ"	Anarchy: All nodes act as distinct CAs	MOCA + PGP-A	Move close for exchange of security credentials	No C, Key = ID
Applicability	Aim	PD TCA	PD TCA	PD TCA	FD TCA	FD TCA	FD CA	PD CA	MOB-a: Off-line CA MOB-so: FD TCA	Threshold PKG
	Net	Planned	Planned	Planned	Planned/ Self-org.	Self-org.	Self-org.	Planned/ Self-org	MOB-a: Planned MOB-so: Self-org.	Planned/ Self-org
Security	Authentication	Off-line	Off-line	Off-line	Off-line	Off-line	Off-line	Off-line	Off-line/side channel	Off-line
	Intrusion tol.	Good	Good	Good	Fair	Fair/Good	Limited	Limited/Fair	Good	Good
	Trust Mnmt	CA	CA	CA	CA: *k**1-hop neighbors	CA: *k* 1-hop neighbors	Nodes	CA + CA certified nodes	MOB-a: N (Off-line CA) MOB-so: Nodes	PKG
	Vulnerabilities	Combiner, CRL distrib, CA key update	CRL distrib, CA key update	CRL distrib, CA key update	CRL distrib, 1-hop neighbors < *k*, (Sybil attack), CA key update	Regional changes, Revocation CRL distrib 1-hop neighbors < k, CA key update	Compromised nodes, CRL distrib	Compromised nodes, Distributed trust mnmt, CRL distrib, CA key update	Revocation, Delay due to restriction on Security credential exchanges, CA key update	IRL distrib, PKG key update
Robustness	Availability assumptions	RP, #CA srvrs > k, Combiner, CA srvrs conn., sync	RP, #CA srvrs > k, CA srvrs conn., sync	RP, #CA srvrs > k, CA srvrs conn., sync	#1-hop neighbors > k, sync	#1-hop neighbors from same region > k, Region-awareness	RP, Chains of trust, sync	#CA srvrs > k or CA certified neighbor > 1	MOB-a: off-line CA MOB-so: side channel	#PKG nodes > k, PKG node conn., sync
	Byz. behavior & Faulty nodes	Good	Good	Good	Good	Limited	Good	Limited	Good	Good
	Group changes	C + CRL	C + CRL	C + CRL	C + CRL	C + CRL/ accusations + Region size	C + CRL	C (+ CRL)	C + CRL	IRL
Scalability		Poor	Limited	Limited	Fair	Limited	Poor	Limited	Limited	Fair

#: The number of, Byz..: Byzantine, C: Certificate, CA: Certificate Authority, CRL: Certificate Revocation List, conn.: Connectivity, distrib: Distribution, FD: Fully distributed, IRL: ID (Key) revocation list, k: threshold value, mnmt: management, N: No/none, PD: Partially distributed, PKG: Private Key Generator, RP: Already running routing protocol, srvrs: Servers, sync: synchronization, TCA: Threshold CA, tol.: tolerance

Table 2: Summary of Public Schemes

5. ENHANCED AUTONOMOUS KEY MANAGEMENT SCHEME

Key management within a Mobile Ad hoc Network (MANET) is a security issue that cannot be ignored. Many researchers have dedicated themselves to this field since 1999. Some schemes are suitable for a limited number of nodes and are inefficient, insecure, or unreliable when the nodes increase. Nodes may join the MANET and leave later normally. Thus, the key management scheme in MANET must be dynamic. The main challenge of MANET is that node handles the joining or leaving of nodes with the limited resources, such as CPU computation, storage, and power consumption [31]. The mobility of a MANET increases its unreliability and limits the bandwidth of wireless environment due to frequent topology changes.

5.1 Autonomous Key Management (AKM)

Autonomous key management (AKM) for a mobile ad hoc network with a large number of nodes is based on a hierarchical structure to provide flexibility and adaptively. Every leaf node in the logical tree structure is a real ad hoc device, and the other nodes are virtual nodes. The root node holds the global secret key, and AKM distributes key shares to its children recursively from the root down to the leaves using Shamir's secret sharing scheme.

		PSGK	SKiMPy	S-HEAL	LKH	PRE	SPINS	GKMPAN	PEBL	INF	LEAP
	Character-istics	Pre-shared group key	Establish key on network formation	Polynomi-al sharing	Key Hierarchy	Proba-bilistic key distribu-tion	Suite of protocols for WSN. Key management: Pre-shared keys between nodes and base station	PRE + µTES-LA assisted revocation for PSGK in WSN	Keys for application and network layer -based on PSGK	Whisper key to neighbor	Resists intrusion through non-mobile nodes
Applicability	Aim	GK	GK	Rev & re-key**)	Rev & re-key**)	Keys between subsets of 1-hop neighbors	PK and Authen-ticated route to base station	GK, rev & re-key	GK	Keys between 1-hop neigh-bors	GK, PK, cluster keys
	Net	Plan	Plan	Plan	Plan	Plan	Plan	Plan	Plan	S. O.	Plan
Security	Authenti-cation	Off-line	C, KP	N	KP	KP	Off-line, µTESLA	KP µTESLA	KP	N	KP
	Intrusion tol	Poor	Limited	Fair	Fair	Fair	Fair	Limited	Poor	Poor	Limited
	Trust Mnmnt	Off-line	Off-line/ special nodes	G Mngr	G Mngr	Controller node	Base station	On-line Key Server	Off-line	N	Base sta-tion
	Vulnerabili-ties	Tamper	Tamper, Rev,CA, Periodic key updates	G Mngr, colluding nodes>t, Byz nodes	GMngr, Byz nodes	Controller node	Base station, Synch	Key Server, synch, Byz nodes, rev of innocent	Tamper, Re-key, synch, Cluster head selection	Eaves-drop-ping	Initial key, Node mobility, Base station
Robustness	Availability assump-tions	N	N	G Mngr, Reliable key distri-bution	G Mngr, Reliable key dis-trib.	Key ring fits with neighbors'	Base station	Key Server	Synch, Full connectivity during TEK establishment, Cluster head	1-hop neigh-bors> 1	No mobility
	Byz. behavior & Faulty nodes	Good	Fair	Poor	Poor	Good	Good	Limited	Limited	Good	Limited
	Dynamic group changes	N	N	Re-key	Re-key	Key re-adver-tising	N	Re-key	Periodic TEK update	N	Re-key
Scalability	Resource efficiency	Good	Fair	Fair	Fair	Limited	Poor	Fair	Limited	Good	*)

Byz: Byzantine, C: Certificate, CA: Certificate authority, G: Group, GK: Group key (symmetric), KP: Key Possession, Mnmt: Management Mngr: manager, N: No/none/Not addressed, PK: Pairwise keys, PKI: Public key infrastructure, Plan: planned, Re-key: re-keying, rev: revocation, S.O.: self organizing, synch: synchronization, TEK: Traffic Encryption Key, WSN: Wireless Sensor Network,

*) assumes static nodes — scalability in MANETs with mobile nodes makes little sense
**) It is here assumed a pre-distributed group key and S-HEAL/LKH used for revocation

Table 3: Summary of Symmetric Key Management Schemes

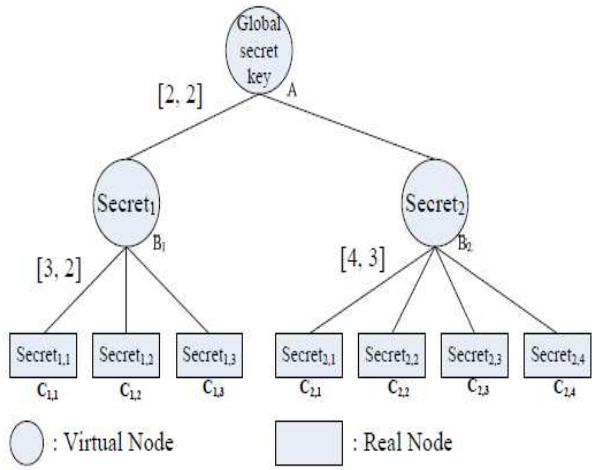

Figure 3: Example of AKM

Every node except the AKM root node must store its own public key pair and its parent node secret share. The secret share each virtual branch node holds is as the secret key, and the public key can be generated using any asymmetric cryptographic scheme, such as RSA. Additionally, every real node has its PKI key pair before joining AKM.

5.1.1 Function Updates

Function update prevents any intruders from compromising the secret, and the AKM updates keys periodically. First, the region with (n, t)-threshold must select t nodes and each node is indicated as node i ∈ 1, . . ., t.

Each node i generates update share Si,j($1 \le j \le n$) of key 0. The node i selects random numbers xj($1 \le j \le n$) and rd($1 \le d \le i - 1$) to compute coefficients ad = (rd|0)($1 \le d \le t - 1$). Si,j = a(xj = Pt−1 r=0 ar(xj)r (mod p), for $1 \le j \le n$. Node i then distributes Si,j to node j ∈ 1, . . . , n. When node j receives the update shares distributed from other t nodes in the region, it computes a new share

$$S'j = Sj + t\ Xi=1Si,j \pmod{p} \quad \ldots\ldots (1)$$

The previous section describes how AKM can manage its secret sharing hierarchical structure using seven region-based functions. These operations cover all possible region changes from node joining to leaving. The key update frequency in MANET is adjustable depending on the application environment. If the frequency is high, the MANET would be secure enough against adversaries, but would result in lower performance and heavy power consumption. On the contrary, if the frequency is low, the communication between nodes in MANET suffers from key inconsistency after many nodes join and leave continuously.

5.1.2 Function Join

Function Join is used when a node i wants to join a (t, n)-threshold region. The node sends a request to node j ∈ 1, . . . , t in the region. Upon receiving the request, node j checks its certificate revoking list (CRL) first. If node j accepts the request, it computes a partial share S′ j of node i:

$$S'_j = S_j l_j(i) + \Delta_j \pmod q \quad (2)$$

Where

$$l_j(i) = \prod_{r=1, r\neq j}^{t} \frac{ID_i - ID_r}{ID_j - ID_r} \pmod q, \quad \Delta_j = \sum_{r=1, r\neq j}^{t} \sigma(j-r) S_{j,r} \quad (3)$$

that Sj,r is a number which pairs of nodes (j, r) ∈ 1 ≤ j ≤ t, 1 ≤ r ≤ t, and

$$\sigma(x) = \begin{cases} 1, & x > 0 \\ -1, & x < 0 \\ 0, & \text{otherwise} \end{cases}$$

After receiving all partial shares, node i generates its secret share Si:

$$S_i = \sum_{j=1}^{t} S'_j = \sum_{j=1}^{t} S_j l_j(ID_i) + \sum_{j=1}^{t} \Delta_j \pmod q. \quad (4)$$

5.1.3 Function Leave

Function leave is used when a node leaves a region. Any node *j* removes the certificate of node *i* from its key management records when receiving a leave request from node *i* or detecting the node leaves. The share key of node *j* does not change until the AKM updates key periodically.

5.1.4 Function Merge

Function merge is used when the number of nodes in a region is below threshold. The region is simply divided into many parts and they join to the other sibling regions respectively.

5.2 Enhanced AKM

The existing AKM uses a RSA algorithm as a public key cryptosystem. Recent years finding the possible alternative to RSA as ECC (Elliptic Curve Cryptography) [32]. All the aspects of cryptographic operations such as encryption, decryption, key exchange and digital signature, ECC is found a good alternative one. ECC uses vey smaller key than RSA and DSA algorithm. For example, the key size of 128 in ECC is more powerful than 1024 bits of RSA in various aspects. Since the MANET is operating mostly on limited resources, we need efficient security mechanism but as simple as possible. It is found ECC is a best suitable algorithm for MANET.

5.2.1 Implementation of Enhanced AKM

The standard simulator ns-2 is used to test the proposed scheme and the obtained result is given in Table 4.

	Communication Time (100 nodes)	Communication Time (150 nodes)
AKM	2.5 ms	3.7 ms
Modified AKM	2.1 ms	3.5 ms
Enhanced AKM	1.79 ms	2.9 ms

Table 4: Comparison of Enhanced AKM with existing works

From the above table, it is found that replacement of RSA by ECC reduces the communication time in a Group key management in MANET. This may be better when the number of nodes increases in large.

5.2.2 Analysis of Enhanced AKM with Existing AKM

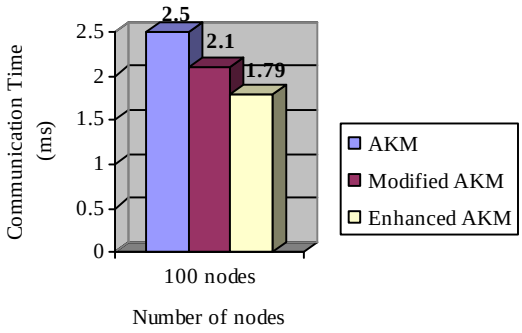

Figure 4: Analysis of Enhanced AKM with 100 nodes

From the above Figure, it is found that replacement of RSA by ECC reduces the communication time in a Group key management in MANET. This may be better when the number of nodes increases in large. The 100 nodes take the communication time of Enhanced AKM is 1.79 ms.It is low communication time compare with existing AKM.

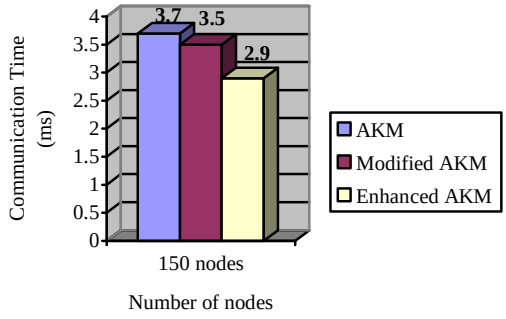

Figure 5: Analysis of Enhanced AKM with 150 nodes

From the above Figure, it is found that the 150 nodes take the communication time of Enhanced AKM and 2.9 ms.It is low communication time compare with existing AKM.

6. CONCLUSION AND FUTURE ENHANCEMENT

In the information age, cryptography enables us to store sensitive information or transmit it across insecure networks like Internet. Exchange of keys among the communication party is one of the greatest challenges. Group key management in mobile ad hoc network (MANET) includes activities for establishment and maintenance of the group key. Maintenance activities consist of changing the group key due to group member's addition or exclusion or due to the use of the group key for long periods of time (key refresh). A good key management policy is extremely important for the deployment of security services. The major categories of group key management schemes are contributory and distributive. Distributive scheme is further classified as public key schemes and symmetric key schemes.

In this research work initially various group key management schemes in both contributory and distributive are studied in all the aspects and comparison is provided. Even though many contributions and open problems are still available in the discussed schemes, the AKM is considered for the enhancement. Recent years finds ECC is a best suitable alternate for any other existing pubic key cryptographic algorithms such as RSA, DSA and DH. To enhance the group key operations of AKM, we have considered ECC instead of RSA. The result obtained after the simulation shows that the enhanced AKM provides better communication time than the existing. Since the applications of MANET is increasing day by day, still many areas of cryptography need to be improved to provide secure communication among nodes.

REFERENCES

[1]. Whitfield Diffie and Martin E. Hellman. New Directions in Cryptography. IEEE Transaction on Information Theory, November 1976, 22(6): 644-654.

[2]. M. Steiner, G. Tsudik, and M. Waidner, "Diffie-Hellman key distribution extended to group communication," in The Proceedings of the 3rd ACM conference on Computer and communications security, pp. 31-37. ACM Press,1996.

[3]. I. Ingemarsson, D. Tang, and C. Wong, "A confer-ence key distribution system," IEEE Transactions on Information Theory, vol. 28, no. 5, pp. 714-720, Sep.1982.

[4]. Mike Burmester and Yvo Desmedt. A Secure and Scalable Group Key Exchange System.

Information Process Letter, 2005, 94(3): 137-143. Original version appears in the proceedings of EUROCRYPT'94, LNCS 950, pp. 275-286.

[5]. M. Burmester and Y. Desmedt. A Secure and Efficient Conference Key Distribution System. In Advances in Cryptology – EUROCRYPT'94, volume 950 of Lecture Notes in Computer Science, pages 275–286. Springer, May 1994.

[6]. M. Burmester. On the risk of opening distributed keys. In Advances in Cryptology {CRYPTO'94, pages 308{317, 1994.

[7]. Pereira et al. A Security Analysis of the Cliques Protocols Suites. In 14-th IEEE Computer Security Foundations Workshop. IEEE Press, June 2001. Available online athttp://citeseer.ist.psu.edu/pereira01security.htm

[8]. Michael Steiner, Gene Tsudik, and Michael Waidner. CLIQUES: A New Approach to Group Key Agreement. In Proceedings of the 18th International Conference on Distributed Computing Systems (ICDCS'98), pages 380–387.IEEE Computer Society Press, 1998.

[9]. R. Clayton, M. Bond, *Experience using a Low-Cost FPGA Design to Crack DES Keys*, in the proceedings of CHES 2002, Lecture Notes in Computer Sciences, vol 2523, pp 579-592, Redwood City, USA, August 2002, Springer-Verlag.

[10]. A.Menezes, P. Van Oorschot, and S. Vanstone. Handbook of applied cryptography. CRC Press series on discrete mathematics and its applications.CRC Press, 1996. ISBN 0-8493-8523-7.

[11]. K.Becker and U.Wille, "Communication complexity of group key distribution," in Proceedings of the 5th ACM Conference on Computer and Communications Security, San Francisco, California, United States, 1998.

[12]. Y. Kim *et al.*, "Communication-efficient group key agreement," in Proceedings of the 16th International Conference on Information

[13]. Y. Kim *et al.*, "Group Key Agreement Efficient in Communication,"*IEEE Trans. Compute.*, vol. 53, pp. 905-921, 2004.*Security: Trusted Information: The New Decade Challenge*, Paris, France, 2001, pp. 229 - 244.

[14]. Bing Wu, Jie Wu and Yuhong Dong,"An efficient group key management scheme for mobile Ad hoc network", International Journal and Networks, Vol. 2008.

[15]. ThairKhdour, Abdullah Aref, "A Hybrid Schema Zone-Based Key Management for MANETS", Journal of Theoretical and Applied Information Technology, vol. 35 No.2,2012.

[16]. Aziz, B., Nourdine, E. and Mohamed, E., "A Recent Survey on Key management Schemes in MANET"ICTTA'08, pp. 1-6, 2008.

[17]. Wu, B., Wu, J., Fernandez, E., Ilyas, M. and Magliveras, S.(2005) 'Secure and efficient key management in mobile adhoc wireless networks', Appears in *Journal of Network and Computer Applications (JNCA)*, Vol. 30, pp.937–954.

[18]. Steer, D., Strawczynski, L., Diffie, W. and Wiener, M. (1990)'A secure audio teleconference system', *Advances in Cryptology – CRYPTO'88*, pp.520–528.

[19]. A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," *Proc. CRYPTO '84*, 1984, pp. 47–53.

[20]. S.A. Camtepe, and B. Yener, "Key Distribution Mechanisms for Wireless Sensor Networks: A Survey," Tech. Report TR-05-07, Rensselaer Polytechnic Institute, 2005.

[21]. S. Rafaeli, and D. Hutchison, "A Survey of Key Management for Secure Group Communication," *ACM Computing Surveys*, vol. 35, no.3,Sep. 2003, pp. 309–29.

[22]. D. Djenouri, L. Khelladi, and N. Badache, "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks," *IEEE Commun. Surveys & Tutorials*, vol. 7, no. 4, 4th Quarter 2005.

[23]. M. Steiner, G. Tsudik, and M. Waidner, "Key Agreement in Dynamic Peer Groups," *IEE* Trans. Parallel and Distributed Syst., vol. 11, no. 8, Aug. 2000, pp. 769–80.

[24]. L. Chen, and C. Kudla, "Identity-Based Authenticated Key Agreement Protocols from Pairings," HP Tech. Report HPL- 2003-25, 2003.

[25]. Y. Wang, "Efficient Identity-Based and Authenticated Key Agreement Protocol," *Cryptology eprint Archive*, Report 2005/108, 2005.

[26]. L. Zhou and Z. J. Haas,"Securing Ad Hoc Networks," *IEEE Network Mag.*, vol. 13, no.6, Nov./Dec. 1999, pp. 24–30.

[27]. A. Shamir, "How to Share a Secret," *Commun. ACM*, vol. 22, Nov. 1979, pp. 612–613.[33 Y. G.Desmedt, "Threshold Cryptography," *European Trans. Telecommun.*, vol. 5, no. 4, July 1994, pp. 449–57.

[28]. Herzberg *et al.*, "Proactive Secret Sharing or: How to Cope with Perpetual Leakage," *Proc. Crypto'95*, 1995, pp. 339–52.

[29]. B.Zhu *et al.*, "Efficient and Robust Key Management for Large Mobile Ad Hoc Networks," *Computer Networks*, vol. 48, no. 4, July 2005, pp.657–82.

[30]. S.Yi, and R. Kravets, "MOCA: MObile Certificate Authority for Wireless Ad Hoc Networks," Report No. UIUCDCS-R-2004-2502, UILU-ENG-2004-1805, University of Illinois at Urbana-Champaign, 2002.

[31]. Yang, H.—Luo, H.—Ye, F.—Lu, S.—Zhang, L.: Security in Mobile Ad Hoc Networks Challenges and Solutions. IEEE Wireless Communications, Vol. 11, 2004, No. 1, pp. 38–47.

[32]. Lauter, K.: The Advantages of Elliptic Curve Cryptography for Wireless Security. IEEE Wireless Communications, Vol. 11, 2004, No. 1, pp. 62–67.

[33]. J. Kong *et al.*, "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks," *Proc. 9th Int'l. Conf. Network Protocols (ICNP'01)*, 2001, pp. 251–60.

[34]. S. Capkun, L. Buttyán, and J. P. Hubaux, "Self-Organized Public- Key Management for Mobile Ad Hoc Networks," *IEEE Trans.Mobile Computing*, vol. 2, no.1, Jan.–Mar. 2003, pp. 1–13.